бится не только указать диаметры оснований и высоту, но также добавить три картинки – по одной для каждого из двух оснований, и ещё одну для боковой поверхности [4].

Frame markers – это маркер в виде специально подготовленной рамки, которая больше похожа на штрих-код. В такую рамку можно поместить любую картинку. Данный вид маркеров отлично подходит в случае, если картинка не была достаточно детализирована [4].

В библиотеку Vuforia встроено ещё и распознание текста, поэтому любое слово или их сочетание может являться маркером. На данный момент поддерживается только латиница [4].

В данной работе был выбран тип маркеров – Image targets. В зависимости от количества маркеров, необходимых для приложения, их можно хранить либо в Device Database, всегда иметь к ним доступ и распознавать их непосредственно на самом устройстве, либо переложить часть этой нагрузки на Cloud Databases – сервис из набора Vuforia Web Services, предназначенный для хранения маркеров и определения их на основании присланных с устройства данных. Оба подхода имеют свои достоинства и недостатки. Определившись с целями создаваемого приложения, был выбран первый подход, т.е. хранить описание маркеров непосредственно в приложении.

Разработанное мобильное приложение с использованием технологии дополненной реальности в программной инженерии может стать новой формой продвижения коммерческого успеха компании и привлечения внимания потенциального потребителя, партнера или заказчика.

Список литературы

1. Сальников И.И. Перспективы развития средств реализации информационных потребностей человека. Успехи современного естествознания. – 2014. – №10. – С.71-73.

2. Дополненная реальность [Электронный ресурс] // Дополненная реальность-будущее сегодня: [сайт]. [2015]. – URL: http://habrahabr.ru/hub/augmented_reality/ (Дата обращения: 09.10.2015).

3. Хусаинов М.А. Перспективы использования дополненной реальности в образовании [Электронный ресурс] // Дополненная реальность в будущем: [сайт]. [2015]. – URL:http://www.vr–online.ru/content/perspektivy–ispolzovanija–dopolnennoj–realnostiobrazovanii–1065 (Дата обращения 22.09.2015).

4. Будущее разработчиков [Электронный ресурс] // «Дополненная реальность» становится просто реальностью: [сайт]. [2015]. – URL: http://crackfiles.ucoz.com/news/dopolnennaja_realnost_stanovitsja_prosto_realnostju/2011–10–16–7// (дата обращения 16.09.2015).

Секция «Безопасность информационных технологий», научный руководитель – Валиев М.М., д-р техн. наук, профессор

К ВОПРОСУ О МОДЕЛИРОВАНИИ УГРОЗ ПЕРСОНАЛЬНЫМ ДАННЫМ ПОЛЬЗОВАТЕЛЕЙ В СИСТЕМАХ ДИСТАНЦИОННОГО ОБУЧЕНИЯ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ

Хлыстова Д.А., Попов К.Г.

Башкирский государственный университет, Уфа, e-mail: popovkg@mail.ru

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Согласно нормативным документам Федеральной службы по техническому и экспортному контролю, носители ПДн могут содержать информацию, представленную в следующих видах:

• акустическая (речевая) информация (РИ), содержащаяся непосредственно в произносимой речи пользователя ИСПДн при осуществлении им функции голосового ввода ПДн в ИСПДн, либо воспроизводимая акустическими средствами ИСПДн (если такие функции предусмотрены технологией обработки ПДн), а также содержащаяся в электромагнитных полях и электрических сигналах, которые возникают за счет преобразований акустической информации;

• видовая информация (ВИ), представленная в виде текста и изображений различных устройств отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн;

• информация, обрабатываемая (циркулирующая) в ИСПДн, в виде электрических, электромагнитных, оптических сигналов;

• информация, обрабатываемая в ИСПДн, представленная в виде бит, байт, файлов и других логических структур.

В целях формирования систематизированного перечня УБПДн при их обработке в ИСПДн и разработке на их основе частных моделей применительно к конкретному виду ИСПДн угрозы классифицируются в соответствии со следующими признаками:

• по виду защищаемой от УБПДн информации, содержащей ПДн;

• по видам возможных источников УБПДн;

• по типу ИСПДн, на которые направлена реализация УБПДн; по способу реализации УБПДн; по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн);

• по используемой уязвимости; по объекту воздействия.

По видам возможных источников УБПДн выделяются следующие классы угроз:

• угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн (внутренний нарушитель);

• угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (внешний нарушитель).

Кроме того, угрозы могут возникать в результате внедрения аппаратных закладок и вредоносных программ. По типу ИСПДн, на которые направлена реализация УБПДн, выделяются следующие классы угроз:

• угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе автономного автоматизированного рабочего места (АРМ);

• угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе АРМ, подключенного к сети общего пользования (к сети международного информационного обмена);

• угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена);

• угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем

с подключением к сети общего пользования (к сети международного информационного обмена);

• угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе распределенных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена).

Итак, способами реализации угроз безопасности могут быть несанкционированный доступ к информации, утечка по техническим каналам, а также специальные воздействия на персональные данные либо информационную систему.

Базовая модель угроз безопасности персональных данных утверждена Приказом ФСТЭК от 15 февраля 2008 г. Угрозы несанкционированного доступа к персональным данным, обрабатываемым в информационной системе, могут осуществляться при помощи программных и аппаратно-программных средств. При этом происходит нарушение режима конфиденциальности в отношении персональных данных путем их неправомерного копирования и/или распространения. Также защищаемые персональные данные могут быть изменены или уничтожены нарушителем, что может также повлечь собой значительные последствия. В ходе реализации угрозы несанкционированного доступа могут быть созданы нештатные режимы работы операционной среды или программного обеспечения, которые возможно будут использованы нарушителем для кражи информации либо воздействия на нее извне.

При реализации угрозы безопасности злоумышленником могут использоваться различные уязвимости, в том числе недостаточный уровень защиты, несовершенство системного и прикладного программного обеспечения, а также протоколов сетевого взаимодействия информационной системы.

Другим видом угроз безопасности персональных данных являются угрозы, реализуемые при помощи технических каналов, таких как утечка речевой, видовой информации, содержащей персональные данные, утечка персональных данных, обрабатываемых в информационных системах, по каналу электромагнитных излучений и наводок. Такие угрозы целесообразно рассматривать в отношении информационных систем высшего класса, в которых обрабатываются специальные категории персональных данных, касающиеся национальной и расовой принадлежности человека, его религиозных либо философских убеждений, здоровья и интимной жизни. Для таких систем разрабатывается специальная модель угроз, при составлении которой анализируются отдельные уязвимости и угрозы, вычисляется их актуальность, определяется достаточность существующих и необходимость дополнительных методов защиты.

Согласно ГОСТ Р 50922-2006 – «Защита информации. Основные термины и определения»: «Модель угроз (безопасности информации) – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации».

Итак, модель угроз – это документ, тем или иным способом описывающий возможные угрозы безопасности персональных данных. Модель угроз безопасности персональных данных необходима для определения требований к системе защиты. Без модели угроз невозможно построить адекватную (с точки зрения денежных затрат) систему защиты информации, обеспечивающую безопасность персональных данных.

В соответствии с пунктом 2 статьи 19 ФЗ «О персональных данных» обеспечение безопасности персональных данных достигается, в частности определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных, т.е. разработкой модели угроз.

Опираясь на приказ ФСТЭК России от 18 февраля 2013 г. № 21 и банк данных угроз, сформированный ГНИИИ ПТЗИ ФСТЭК России, представляется возможным выделить самые актуальные угрозы для системы дистанционного образования образовательных организаций:

• угроза изменения компонентов системы;

• угроза несанкционированного доступа к аутентификационной информации;

• угроза несанкционированного удаления защищаемой информации;

• угроза аппаратного сброса пароля BIOS;

• угроза внедрения вредоносного кода в BIOS;

• угроза внедрения кода или данных.

На базе этих основных угроз будет строится модель угроз, но нельзя оставлять без внимания проблему раскрытия паролей, что также является прямой угрозой в данной сфере.

Есть много способов решить эту проблему, но самый качественный, на наш взгляд, это ввод персональных средств криптографической защиты информации и двухфакторной модели аутентификации в данную сферу образования.

Список литературы

1. Федеральный Закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» (ред. от 21 июля 2014 года) [Официальный сайт компании «КонсультантПлюс»].

2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.) [Официальный сайт ФСТЭК России].

Секция «Государственная система учета недвижимого имущества: тенденции развития», научный руководитель – Комкова А.В.

ГОСУДАРСТВЕННЫЙ КАДАСТР НЕДВИЖИМОСТИ: ПРОЦЕССУАЛЬНЫЕ АСПЕКТЫ ЗАЩИТЫ ИНТЕРЕСОВ ПРАВООБЛАДАТЕЛЕЙ ЗЕМЕЛЬНЫХ УЧАСТКОВ

Анисина З.А., Комкова А.В.

Московский государственный университет путей сообщения (МИИТ), Москва, e-mail: Zlata.anisina@mail.ru

Согласно проведенным исследованием статья 7 Федерального закона «О государственном кадастре недвижимости» (редакция, действующая с 1 декабря 2015 года) устанавливает состав сведений об объекте недвижимости.

В частности, к таким сведениям относятся описание местоположения границ объекта недвижимости, если объектом недвижимости является земельный участок, и площадь земельного участка. Эти характеристики являются уникальными, т.к. позволяют идентифицировать объект недвижимости.

Перед правообладателем ранее учтенного земельного участка встает необходимость внести в кадастр недостающие сведения о его границах.

В соответствии со ст. 22 ФЗ «О государственном кадастре недвижимости» (с изм. и доп., вступ. в силу с 01.12.2015) сведения государственного кадастра недвижимости об уникальных характеристиках земельного участка (описание местоположения границ и площадь) могут быть изменены только на основании Заявления и Межевого плана, а также в случае, предусмотренном ч. 14 ст. 45 указанного Закона, в со-